La tronçonneuse et le faucon (Chainsaw & Hayabusa)

Jean-Marc Pouchoulon

Novembre 2025

L'idée de ces outils est de réaliser des recherches directement sur des fichiers EVTX en utilisant les règles Sigma pour rechercher des motifs d'intrusion dans les logs. Ecrit en Rust, ils sont particulièrement rapides, efficaces et évolutifs par la prise en compte de nouvelles règles Sigma. On se propose dans ces TD de les utiliser pour rechercher des attaques dans des fichiers EVTX [1].

1 Chainsaw

Installation de Chainsaw

Vous pouvez chargez la dernière "release" de Chainsaw ici : `https://github.com/WithSecureLabs/chainsaw/releases` et la mettre dans /usr/local/bin/chainsaw.

A la maison, vous pouvez compiler l'outil:

```
git clone https://github.com/countercept/chainsaw.git
cd chainsaw
cargo build --release
cd target/release
sudo cp ./chainsaw  /usr/local/bin
```

Créez une directory de travail:

```
mkdir chainsaw_workdir
cd chainsaw_workdir
git clone https://github.com/countercept/chainsaw.git
# installez les fichiers EVTX témoins
git clone https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.git
# installez les règles Sigma
git clone https://github.com/SigmaHQ/sigma.git
```

Si votre version de Rust est trop ancienne, installez une version plus récente de rustc::

1. mis à disposition par Samir Bousseaden

```
# sous test dé-sinsallation de rustc
sudo apt remove rustc
# puis installation locale
curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
....
```

Utilisation de Chainsaw

Aidez-vous de la documentation afin de répondre aux questions suivantes:

1. Faites une "chasse" globales des attaques sur tous les extraits EVTX_SAMPLES.
2. Recherchez les "events" relatifs à "Mimikatz" dans les fichiers EVTX_SAMPLES.
3. Recherchez les "events" relatifs au "scripts block logging entry" qui caractérisent le lancement d'un script Powershell.
4. Recherchez les "events" relatifs à la création d'un process.
5. Recherchez les "events" relatifs à l'URL 'DC[0-9].insecurebank.local'. Faites-en une sortie au format JSON et "pipez" la sortie vers 'jq'.
6. Téléchargez les trois fichiers EVTX sur Moodle et faites une recherche d'attaques.

2 Hayabusa

Installation d'Hayabusa

Téléchargez le binaire Hayakusa sur Moodle et placez le dans /usr/local/bin/hayabusa.

A la maison, vous pourrez le compiler ainsi :

```
sudo apt install musl-tools libssl-dev
rustup install stable-x86_64-unknown-linux-musl
rustup target add x86_64-unknown-linux-musl
git clone https://github.com/Yamato-Security/hayabusa.git --recursive
cd hayabusa
cargo build --release --target=x86_64-unknown-linux-musl
cp ./target/x86_64-unknown-linux-musl/release/hayabusa /sur/local/bin/hayabusa
chmod +x /usr/local/bin/hayabusa
```

1. Utilisez Hayabusa afin d'obtenir la répartition des différents "events" par ID sur les deux channels security et sysmon.
2. Utilisez Hayabusa afin d'obtenir les "logons" réussis ou pas.
3. Trouvez le TOP 10 des "events" les plus fréquents sur l'ensemble des fichiers EVTX-ATTACK-SAMPLES.
4. Trouvez les "events" relatifs à "Mimikatz" sur l'ensemble des fichiers "security", "sysmon" et "forwarded".
5. Exportez-les au format "multiline json" et utilisez **Nushell** avec l'option **from json –objects** pour l'afficher sous forme d'un tableau. Vous pouvez installez Nushell avec les commandes suivantes:

   ```
   mkdir -p /tmp/docker-nushell && cd /tmp/docker-nushell
   wget https://raw.githubusercontent.com/nushell/nushell/refs/heads/main/docker/Dockerfile -O Dockerfile
   docker build --no-cache . -t nushell-latest
   docker run -it nushell-latest -c "plugin list | get name"
   ```

6. Donnez le top 10 des "events" les plus fréquents dans ce tableau.

3 Bonus

Utilisez Chainsaw et Hayabusa sur les logs EVTX générées lors du TP "WEC".